REMARKS

Claims 1-27 were pending and presented for examination. In an Office Action dated May 4, 2007, claims 1-27 were rejected. Applicant is canceling claims 20-23 and amending claims 1, 6, 14, 17-18, and 24 in this Amendment and Response. These changes are believed not to introduce new matter, and their entry is respectfully requested.

In view of the Amendments herein and the Remarks that follow, Applicant respectfully requests that Examiner reconsider all outstanding objections and rejections, and withdraw them.

Response to Rejection Under 35 USC § 101

In the Office Action, Examiner has rejected claims 1-19 and 24-26 under 35 USC § 101, as allegedly being directed to non-statutory subject matter. This rejection is respectfully traversed as applied to the amended claims.

Examiner states that claims 1 and 6 could be reasonably drawn to functional descriptive material per se and may be taken to mean software alone, and as a result are not directed to statutory subject matter. However, claims 1 and 6 are processes and fall under at least the process category of the four subject matter categories of 35 USC § 101. The claims are not functional descriptive material nor software and recite statutory processes.

Claim 24, as amended, recites "A computer-readable storage medium containing executable computer program instructions for ..." Examiner states that "the modules, when implemented in software residing on a CRM are non-statutory until they are executed ..." This is contradicted by MPEP 2106.01.I., which states that a computer-readable medium encoded with a computer program is statutory because it permits the computer program's

functionality to be realized. Examiner's statement that modules residing on a CRM are not statutory unless executed is incorrect.

Applicant respectfully requests that Examiner withdraw the § 101 rejection to claims 1, 6, and 24, and to dependent claims 2-5, 7-19, and 25-26.

Response to Rejection Under 35 USC § 112, Paragraph 2

In the Office Action, Examiner has rejected claims 5-13 under 35 USC § 112, ¶ 2 as allegedly being indefinite. Examiner states that it is unclear how to determine if code having a decryption loop contains malicious code since the specification defines a decryption loop as a section of malicious code.

Applicant is amending the specification to remove "malicious" from the definition of a decryption loop. As known by people having ordinary skill in the art, a decryption loop is not necessarily malicious, though it is sometimes used in malicious code. The amendment is merely to conform an imprecise definition in the specification with its ordinary meaning, and does not introduce new matter.

As a result, the basis for the § 112 rejection to claims 5, 6, and dependent claims 7-13 is obviated.

Response to Rejection Under 35 USC 102(b) in View of Yamamoto

In the Office Action, Examiner rejects claims 1-4, and 24-26 under 35 USC § 102(b) as allegedly being anticipated by U.S. Patent No. 5,881,151 to Yamamoto ("Yamamoto"). This rejection is respectfully traversed.

As amended, claim 1 recites a computer-implemented method for determining whether computer code contains malicious code, the method comprising:

identifying **computer code suspected of currently containing malicious code**;

optimizing the identified computer code to produce optimized code; and

subjecting the optimized code to a malicious code detection protocol; and

responsive to the malicious code detection protocol detecting malicious code in the optimized code, declaring a confirmation that the computer code contains malicious code.

(emphasis added)

As can be seen, the claim recites identifying computer code suspected of currently containing malicious code and optimizing that computer code to produce optimized code. The optimized code is then subjected to a malicious code detection protocol, and a confirmation of malicious code is declared responsive to detecting malicious code. The claimed invention beneficially optimizes the code to simplify it so that malicious code detection protocols can be more efficiently and effectively applied to the code. For example, a virus may contain intentionally complexified code that makes virus detection protocols slow or inaccurate. The claimed invention first optimizes the code so that the detection protocols can be more successful.

As amended, claim 24 contains similar language to claim 1. All arguments regarding claim 1 presented below apply equally to claim 24.

Claim 1 is not disclosed by Yamamoto. Yamamoto discloses compiling and optimizing a virus-free source program and adding virus diagnosing code to the resulting object code. The virus diagnosing code can be run later to verify that the program has not been modified by a virus subsequent to being compiled. For example, the code can check that the program size has not changed since immediately after the program was compiled (col. 6, lines 37-50). The diagnosing code operates under the assumption that the source

program that is compiled and optimized is free of viruses. Yamamoto is not concerned with optimizing code that is currently suspected of containing malicious code.

Specifically, Yamamoto does not disclose "identifying computer code suspected of **currently containing** malicious code," and optimizing that code to produce optimized code. The Examiner cites col. 4, lines 51-55 which discloses a code optimizing portion 38 of the compiler and col. 5, lines 26-38 which discloses details of optimizations performed by the code optimizing portion 38. However, the optimizing portion 38 is merely part of a standard compiler that converts the source program 10, which must currently be free of malicious code in order for Yamamoto's technique to function, to the object code 16. The optimizing portion 38 does not optimize code that is suspected of currently containing malicious code.

Based on the above remarks, Applicant submits that for at least these reasons claims 1 and 24 and dependent claims 2-4 and 25-26 are patentably distinguishable over the cited reference. Therefore, Applicant respectfully requests that Examiner reconsider the rejection, and withdraw it.

Response to Rejection Under 35 USC 103(a)

In the Office Action, Examiner rejects claims 5-19, and 27 under 35 USC § 103(a). Claims 5-13 are rejected over Yamamoto in view of U.S. Patent No. 5,826,013 to Nachenberg et al. ("Nachenberg"). Claims 14-18 are rejected over Yamamoto in view of U.S. Patent No. 5,734,908 to Chan et al. ("Chan"). Claim 19 is rejected over Yamamoto and Chan in view of U.S. Patent Publication No. 2004/0221279 to Lovett et al. ("Lovett"). Claim 27 is rejected over Yamamoto in view of Lovett. These rejections are respectfully traversed.

Since claims 5 and 14-19, as amended, are dependent on claim 1, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claims 5

and 14-19. Claim 6 contains similar language to claim 1 for optimizing code suspected of containing malicious code. All arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claim 6 and dependent claims 7-13.

Nachenberg, Chan, and Lovett do not remedy the deficiencies of Yamamoto with respect to these arguments. Nachenberg describes a method for detecting a polymorphic virus using emulation. While Nachenberg does mention "[reducing] the number of file instructions that must be emulated in order to determine whether a target file is infected by a virus" at col. 6, lines 57-59, this reducing is not performed through code optimization but rather through various virus exclusion methods as described in col. 6, line 59 to col. 7, line 8. Chan is concerned with source code optimization methods that better utilize resources on the underlying machine. Lovett discloses dead code elimination when translating code from one processor instruction set to another. None of these references are concerned with optimizing code suspected of currently containing malicious code.

Claim 27 recites a method for determining whether computer code contains malicious code, the method comprising:

> performing a dead code elimination procedure on the computer code;
> noting the amount of dead code eliminated during the dead code elimination procedure; and
> when the **amount of dead code eliminated during the dead code elimination procedure exceeds a preselected dead code threshold**, declaring a suspicion of malicious code in the computer code.
> (emphasis added)

As can be seen, the claim recites performing a dead code elimination procedure on the computer code, noting the amount of dead code eliminated during the procedure, and declaring a suspicion of malicious code in the computer code when this amount exceeds a

threshold. The claimed invention enables the detection of suspicious code by determining that the code contains a certain amount of dead code, which is often found in malicious code.

Claim 27 is not disclosed by the combination of Yamamoto and Lovett. As discussed above, Yamamoto discloses optimizing only clean source code, not optimizing computer code to determine if there was malicious code in the computer code prior to the optimization (dead code elimination is a type of optimization). Lovett discloses dead code elimination but is not concerned with declaring a suspicion of malicious code based on the amount of dead code eliminated.

Accordingly, the references do not disclose "when the amount of dead code eliminated during the dead code elimination procedure exceeds a preselected dead code threshold, declaring a suspicion of malicious code in the computer code." Paragraphs [0133], [0144], [0091], and [0098] cited by Examiner merely mention thresholds used in other contexts, such as an execution count threshold for group block generation or a profiling metric threshold for group block construction. These are not thresholds of amounts of dead code, and the thresholds are not used to declare a suspicion of malicious code.

Based on the above remarks, Applicant respectfully submits that for at least these reasons claims 5-19 and 27 are patentably distinguishable over the cited references. Therefore, Applicant respectfully requests that Examiner reconsider the rejection, and withdraw it.

Applicant invites Examiner to contact Applicant's representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,
Frederic Perriot

Date: August 28, 2007 By: /Brian Hoffman/

Brian M. Hoffman, Attorney of Record
Registration No. 39,713
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (415) 875-2484
Fax: (650) 938-5200